Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A system, comprising:

a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network; and

an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic [[or]] from the node, with the aggregator device further comprising:

a process executed on the aggregator device to detect anomalies in connection patterns; and

a process executed on the aggregator device to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies.

2. (Previously Presented) The system of claim 1 wherein the aggregator determines at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusions.

3. (Previously Presented) The system of claim 2 wherein the aggregator further comprises:

a process that collects statistical information on packets that are sent between nodes on a network and which sends the statistical information to the aggregator.

Claim 4 is canceled.

5. (Previously Presented) The system of claim 1 wherein the collector[[s]] devices have a passive link to devices in the network.

Claim 6 is canceled.

7. (Previously Presented) The system of claim 1 wherein the anomalies include unauthorized access and worm propagation.

8. (Original) The system of claim 1 wherein the connection table includes a plurality of records that are indexed by source address.

9. (Original) The system of claim 1 wherein the connection table includes a plurality of records that are indexed by destination address.

10. (Original) The system of claim 1 wherein the connection table includes a plurality of records that are indexed by time.

11. (Original) The system of claim 1 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time.

12. (Original) The system of claim 1 wherein the connection table includes a plurality of connection sub-tables to track data at different time scales.

13. (Previously Presented) The system of claim 12 wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other

sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time.

14. (Currently Amended) A method, comprises:

sending connection information to an aggregator to identify host connection pairs collected from a plurality of collector devices; and

producing in the aggregator a connection table that maps each node on the network to a record that stores information about traffic to the node and traffic [[or]] from the node, with the connection table including a plurality of entries that are indexed by source address.

15. (Previously Presented) The method of claim 14 further comprising:

collecting statistical information in the collector devices to send to the aggregator device.

16. (Previously Presented) The method of claim 15 further comprises:

determining from the connection information and the statistical information occurrences of network anomalies; and

aggregating anomalies into network events that indicate potential network intrusions and communicating occurrences of network events to an operator.

Claim 17 is canceled.

18. (Original) The method of claim 14 wherein the connection table includes a plurality of entries that are indexed by destination address.

19. (Original) The method of claim 14 wherein the connection table includes a plurality of records that are indexed by time.

20. (Original) The method of claim 14 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time.

21. (Original) The method of claim 14 wherein the connection table includes a plurality of connection sub-tables to track data at different time scales.

22. (Previously Presented) The method of claim 21 wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time.

23. (Currently Amended) A computer implemented method of detecting a new host connecting to a network comprises:

receiving by a computer statistics collected from a host in the network; and

indicating by the computer to a console that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T.

24. (Previously Presented) A method executed in a computing device for detecting a failed host in a network comprises:

determining in the computing device, if both a mean historical rate of server response packets from a host is greater than M and a ratio of a standard deviation of historical rate of server response packets from the host to a mean profiled rate of server response packets from the host is less than R over a period of time; and

indicating the host as a potential failed host if both conditions are present.

25. (Previously Presented) The method of claim 23 wherein indicating comprises:

determining the minimal rate of N/T packets/second to avoid false positives caused by scans or spoofing attacks.

26. (Previously Presented) The method of claim 24 wherein indicating comprises:

determining a period seconds of continuous inactivity of the potential failed host to expire the potential failed host after the period of continuous inactivity; and

generating a new host event if the expired failed host sends traffic on the network after the period of continuous inactivity has elapsed.

27. (Previously Presented) The method of claim 24 wherein a host failure indicates an inability by the host to generate traffic on the network or an application failure.

28. (New) A storage medium storing a computer program product, the computer program product comprising instructions for causing a computer to:

collect connection information to identify host connection pairs from packets that are sent between nodes on a network and produce a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node;

detect anomalies in connection patterns; and

aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies.

29. (New) The storage medium of claim 28 further comprising instructions to determine at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusions.

30. (New) The storage medium of claim 28 further comprising instructions to collect statistical information on packets that are sent between nodes on a network.

31. (New) The storage medium of claim 28 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time.

32. (New) The storage medium of claim 28 wherein the connection table includes a plurality of connection sub-tables to track data at different time scales, the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time.

33. (New) A device, comprising:

a processor;

memory associated with the processor; and

a storage medium a computer program product for detecting a new host connecting to a network comprises instructions to:

receive statistics collected from a host in the network; and

indicate to a console that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T.

34. (New) A device, comprising:

a processor;

memory associated with the processor; and

a storage medium a computer program product for detecting a failed host in a network comprises instructions to:

determine if both a mean historical rate of server response packets from a host is greater than M and a ratio of a standard deviation of historical rate of server response packets from the host to a mean profiled rate of server response packets from the host is less than R over a period of time; and indicate the host as a potential failed host if both conditions are present.

35. (New) The device of claim 34 wherein instructions to indicate comprises instructions to:

determine the minimal rate of N/T packets/second to avoid false positives caused by scans or spoofing attacks; and

wherein a host failure indicates an inability by the host to generate traffic on the network or an application failure.

36. (New) The device of claim 34 wherein instructions to indicate comprises instructions to:

determine a period seconds of continuous inactivity of the potential failed host to expire the potential failed host after the period of continuous inactivity; and

generate a new host event if the expired failed host sends traffic on the network after the period of continuous inactivity has elapsed.